



# ASSOCIATION OF AMERICAN RAILROADS

**Law Department**  
Dennis J. Starks  
Senior Commerce Counsel

September 24, 2003

Ms. Marlene H. Dortch, Secretary  
Federal Communications Commission  
445 12th Street SW  
Washington, D.C. 20554

Re: RM No. 10687, Request of Industrial Telecommunications Association to be a  
Certified Frequency Coordinator in the Power, Railroad and Automobile  
Emergency Radio Services

## **NOTICE OF EX PARTE COMMUNICATION**

Dear Ms. Dortch:

Pursuant to Section 1.1206 of the Commission's Rules, I am electronically filing this notice of a written and oral ex parte communication.

Yesterday, the undersigned, on behalf of the Association of American Railroads (AAR), together with Mr. Thomas Keller, also representing AAR, met with members of the Commission's staff to discuss the unanimous and vigorous opposition of the U.S. railroad industry to the request of Industrial Telecommunications Association (ITA) to become a certified frequency coordinator for railroad frequencies under Part 90 of the Commission's rules (RM-10687). Representing the Commission at the meeting were Ms. D'wana Terry, Mr. Herb Zeiler, Mr. Scot Stone and Mr. John Borkowski, of the Public Safety and Private Wireless Division of the Wireless Telecommunications Bureau.

The written portion of our ex parte communication consisted of the presentation of a copy of a newspaper article published on page E-1 of The Washington Post on September 9, 2003, describing how the railroad industry (among others) is managing the risk of terrorist threats in the wake of the attacks of September 11, 2001. Specifically, the article describes the railroad industry's use of the "eyes and ears of experienced...dispatchers, engineers, conductors and maintenance-of-way employees" to help identify security threats, as well as the use of U.S. government intelligence resources tied to AAR's "24-hour command center" in Washington, D.C. A copy of the article is enclosed.

During the meeting, Mr. Keller and I pointed out that the railroad industry's mobile radio network is a critical link in this security system, underscoring more than ever the need for knowledgeable frequency coordination to ensure interference-free communications on railroad mobile radio channels, which could be jeopardized if persons unfamiliar with the complexities of railroad communications were permitted to perform the frequency coordination function.

We also reiterated the rationale behind the critical infrastructure community's strong opposition to ITA's request, as summarized in the joint ex parte presentation given on August 28, 2003 by AAR, the American Automobile Association, the American Petroleum Institute and the Utilities Telecommunications Council to Mr. Bryan Tramont, FCC Chief of Staff, and in the joint ex parte presentation given by the same parties on July 22, 2003, to several staff members of the Public Safety and Private Wireless Division.

That rationale is the same one articulated by the Commission in 1997 when it balanced the benefits of competitive frequency coordination against the potential safety risks resulting from improper coordination decisions by entities that are unfamiliar with the intricacies of critical infrastructure communications. The Commission wisely opted in favor of safety in 1997 by creating a narrowly defined exception to the general rule of competitive frequency coordination, stating that "using coordinators who are knowledgeable with [the] special communications needs [of critical infrastructure] is the best way to protect those operations, which involve safety-related communications, and outweighs any potential benefits that may be gained through a competitive frequency coordination process." (Second Report and Order, 12 FCC Rcd 14307, 14329-30 (1997), emphasis added).

At yesterday's meeting we also discussed some of the many special communications needs of the railroad industry (all of which are described in detail in AAR's "Opposition to ITA's Request" filed on April 23, 2003). As AAR demonstrated in its Opposition (see, e.g., pp. 7-8), a frequency coordinator who is not versed in the specialized attributes of railroad communications could easily make incorrect coordination decisions that could result in denial of service, harmful interference, violation of federal safety requirements for railroad radio use, or other negative consequences. The specialized circumstances of the railroad mobile radio network discussed at the meeting were as follows:

- (1) Consists of a complex nationwide system requiring interoperability among all railroads;
- (2) Subject to comprehensive federal safety regulatory requirements for radio communications (administered by the Federal Railroad Administration);
- (3) Involves intra-industry priorities for channel usage based on functionality (i.e., mainline dispatch, maintenance-of-way; railroad police; defect detector devices, end-of-train devices, etc.);

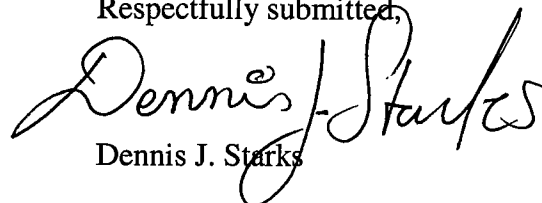
- (4) Uses consensus-based industry standards for radio equipment and nationwide channel plan (especially important for the upcoming industry-wide migration to 12.5 kHz bandwidth technology by U.S. and Canadian railroads);
- (5) Requires frequent cross-border collaboration and consultation on frequency coordination with AAR's Canadian counterpart (Railway Association of Canada);
- (6) Directly linked to homeland security and national security issues (see AAR Opposition, *supra*, at 16-19, and the enclosed Washington Post article).

Finally, we noted at the meeting that ITA appears to have misled the Commission by suggesting at pages 10-12 of its "Comments" filed on May 12, 2003, that ITA is qualified to coordinate railroad channels because it has performed frequency coordinations for "a substantial number" of "railroad eligibles" for their "critical operations." Of the three possible rail-related entities listed among all the examples at pages 10-12 of ITA's Comments (Autorail Services, Canac Industrial Rail Services, and Federal Railroad Administration), none of the three involved train movements, train control, railroad security, or any other "critical operations." Indeed, two were for coordinating localized personnel and car-switching activities (Autorail and Canac) and the third was a mobile application for communicating with employees in office buildings at conventions (Federal Railroad Administration); and all three involved ordinary Industrial/Business channels.

In this regard, we pointed out that, while some railroads use non-railroad channels for ancillary non-critical activities, the mere fact that ITA may have performed frequency coordinations for such uses does not, by any stretch, mean that ITA possesses the specialized knowledge and expertise necessary to coordinate the frequencies designated as "LR" (i.e., railroad channels) in Part 90 of the Commission's rules -- frequencies that are used in the railroad industry for mainline dispatch, onboard links, defect detector devices, railroad security, and the like.

Please feel free to contact the undersigned if there are any questions about this submission.

Respectfully submitted,



Dennis J. Starks

Enclosure

cc: Meeting Participants  
Mr. Bryan Tramont  
Jeremy Denton and Robin Landis, ITA

## Adding Protection Without Disruption

Challenge Looms for Carriers, Government

By Don Phillips

Washington Post Staff Writer

Tuesday, September 9, 2003; Page E01

When the United States began bombing al Qaeda camps in Afghanistan in October 2001, the railroad industry voluntarily suspended deliveries of dangerous chemicals to avoid possible terrorist reprisals. Within days, however, a shortage of chlorine left the Los Angeles water system within two days of shutting off service to millions of customers.

That was perhaps the first economic object lesson in the post-Sept. 11 era: Absolutely securing every movement of potentially dangerous cargo cannot be accomplished without disrupting the U.S. economy. Even relatively minor delays in the flow of goods in an economy that depends on just-in-time deliveries from around the world can cost billions of dollars.

Two years later, government and industry are still struggling with the question of how much they can do to secure the 11 billion tons of cargo -- including 1.5 billion tons of hazardous material -- that move through the United States each year without causing such economic damage that they, in effect, do terrorists' work for them. Complicating the task is the sheer size and openness of the U.S. transportation system: 3.9 million miles of roads, more than 200,000 miles of railroad tracks, 600,000 bridges, 2.2 million miles of pipelines, 5,000 public-use airports and 300 ports, all with vulnerabilities.

"If we impose a security regime that kills an industry, we have failed in our job," said Elaine Dezenski, director of maritime, land and cargo policy for the Transportation Security Administration.

The questions of how much security is possible and reasonable in cargo shipments will come up again today in a Senate Committee on Commerce, Science and Transportation hearing. The House has already passed a proposal by Reps. Edward J. Markey (D-Mass.) and Christopher Shays (R-Conn.) to require screening of all air cargo loaded into the belly of passenger planes, regardless of the cargo's size. Under current rules, only cargo from a list of "known shippers" can be loaded aboard passenger planes, and shipments weighing less than 16 ounces are not subject to any screening.

TSA Administrator James M. Loy and airline industry leaders say no technology now exists to allow screening of all air cargo, and the only choice would be to stop belly cargo shipments -- which the already money-losing airline industry says would cost it \$4 billion in annual revenue and 27,000 jobs. Even if the technology were available to screen all air cargo, it would require the hiring of an additional 8,000 screeners, Dezenski said.

Industry executives say the Markey-Shays proposal is an example of well-intended but hasty reactions that could cause more damage than they prevent. "TSA understands that, and Congress is beginning to understand it, but there's a lot of knee-jerk reaction," said John A. Legler, security director for the American Trucking Associations.

#### **Potential Target Focus**

Loy espouses a "threat-based and risk-managed" approach to security in which cargo moved by legitimate known shippers is only spot-checked, while other cargo receives most of the attention, especially cargo identified as suspect by intelligence agencies.

Loy said his agency is applying lessons learned after the Sept. 11 attacks when legislation requiring more stringent screening of airline passengers and baggage was passed in haste and rules were imposed on tight deadlines, with the government only later facing their impact and how much they would cost.

"You have to draw a distinction between the impulsive reaction after 9/11 in the aviation sector" and cargo movement, Loy said.

John M. Meenan, executive vice president of the Air Transport Association, said the airline industry and the TSA are addressing cargo security concerns by being more careful about whom they accept shipments from, developing better trace technology to spot explosives, making greater use of bomb-sniffing dogs and opening some cargo at random.

Railroads, trucking companies and ports have beefed up security around their facilities with more guards, locks and gates. They have trained employees to watch for and report signs of potential terrorist activity, and worked with intelligence agencies to identify potential threats to their systems.

The TSA is expected to propose new rules this year for further transportation security enhancements. Under the Homeland Security Act passed late last year, criminal background checks will be required for transportation workers who deal with hazardous materials. The TSA also has a number of other security programs in the pipeline, including a universal identity card for all transport workers who require access to secure areas.

But congressional staffers complain frequently that the Department of Homeland Security is in a state of bureaucratic and budgetary confusion, constantly moving money from one program to another. And industry executives complain of receiving contradictory directives from two or more different offices.

The General Accounting Office, in a report prepared for Tuesday's Senate hearing, generally confirmed these complaints and called on the departments of Homeland Security and Transportation to clarify the roles of agencies dealing with transportation security. The GAO report said there has been a "breakdown in communication" between the two agencies.

The industry looks no further than last Independence Day to find an example.

The Homeland Security Act included fireworks among the explosives regulated by the Bureau of Alcohol, Tobacco and Firearms. This led to confusion about whether railroad workers would have to undergo criminal background checks before they began delivering this year's shipments of fireworks.

On Feb. 6, railroads placed an embargo on all fireworks while awaiting clarification, a blow to the fireworks industry because almost all fireworks move by rail. Fireworks manufacturers said they could find only two truck lines that would accept fireworks shipments. For four months, ATF and the Transportation Department wrangled over who had jurisdiction over railroad workers. Only after it became obvious that many July 4 celebrations would have to be canceled did the agencies clarify that fireworks could resume movement. The Transportation Department retained rail worker jurisdiction.

#### **Port Security Ordered**

The TSA, after spending its first year concentrating primarily on airline security, is now turning more of its attention to cargo.

New Coast Guard regulations require ports to perform security assessments and submit detailed security plans by Jan. 1, 2004. The Coast Guard estimates ports will require \$1.1 billion in security investment in the first year alone. But President Bush has sought no funds designated specifically for port security, and Congress appears set to approve \$150 million in the fiscal 2004 budget.

Sens. Ernest F. Hollings (D-S.C.) and Patty Murray (D-Wash.) have accused the administration of failing to pay proper attention to port security. The Department of Homeland Security has already announced about \$340 million in port security grants under earlier port security legislation, but Hollings terms that inadequate and calls some of the grants smoke-and-mirrors.

For instance, Hollings's home port of Charleston was awarded \$3.79 million by homeland security's office of domestic preparedness, but the office designated \$2 million of that for a helicopter for the Charleston County Sheriff's Department, which could be used for Coast Guard officials and other federal agencies. Some time later, however, the department informed the sheriff's office that it could not use the money for a helicopter even though the department made the designation, so the \$2 million could not be spent. Hollings said he is still awaiting an explanation.

In nearby Jacksonville, Fla., the department announced a \$3.4 million grant. It later told the port it could spend \$333,000 on a video security system but not the remaining money, because the terms of the grant, as approved by the department, called for it to be spent for security gates. That would violate department rules, port officials said they were told.

#### **Industry Initiatives**

Amid that confusion, rail and truck lines have been trying to manage risks by moving forward with their own new security systems, using intelligence reports and the eyes and ears of experienced truck drivers, dispatchers, engineers, conductors and maintenance-of-way employees.

The American Trucking Associations and the Federal Motor Carrier Safety Administration are training a corps of selected truck drivers to watch for and report signs of potential terrorism, in addition to dangerous road conditions and accidents.

Already, the program has produced some unintended benefits, ATA's Legler said. For instance, a truck driver thought it was suspicious that he delivered a full marine container to an apartment building. He called his dispatcher, who called police, who made a major drug bust.



The railroad industry has formed a 24-hour command center in Washington and has representatives assigned to the CIA and the FBI intelligence organizations. The industry has done a study to identify vulnerable points in its systems and to set contingency plans for protection during times of threats. Tests are also being conducted at Aberdeen Proving Grounds in Maryland to determine how to strengthen and protect railcars carrying hazardous materials.

"We have had excellent cooperation from the intelligence community," said Chuck Dettman, executive vice president of the Association of American Railroads.

Railroad sources said the railroad security system may have prevented at least one attack. Intelligence agencies reported that a group of suspected terrorists was looking for bridges to blow up in one major city, which the sources did not want to name. The railroad command center immediately dispatched guards to every bridge in the area until the threat passed.

The Customs Service, whose main enforcement responsibility was searching for drugs, has installed equipment at the Mexican and Canadian borders that is proving helpful in looking for terrorist threats, including the Vessel and Cargo Inspection System, which uses gamma ray technology to produce an image of the inside of a truck or rail car. At seven points on the Mexican border and two on the Canadian border, an entire train can be imaged while passing through at 5 to 7 mph.

But government and industry officials agree that, in the end, there is only so much they can do. Unlike airports and ports, trains and trucks operate over many thousands of miles of track and highways that are wide open and too costly to protect mile by mile. "You can't protect all of anything all the time," Dettman said. "But when you reverse the view of what a terrorist's motives are and put that up against what your vulnerabilities are, then you narrow that seemingly impossible task down to make it more manageable."